Australian Banking Association

05 March 2021

Mr Tony Rasman
Public Affairs Manager
The Institute of Internal Auditors
By email: tony.rasman@iia.org.au

Dear Tony

Supplementary Guidance on the Audit of Risk Culture

Risk culture emerged as an element of operational risk from the Global Financial Crisis and has been the focus of regulators globally and in Australia since. Focus on organisational culture was a recommendation from the Royal Commission (Recommendation 5.6), and Australian banks have undertaken significant efforts to improve risk culture. Therefore, the ABA supports the Institute for Internal Auditors' (**IIA**s) efforts to develop a risk culture audit guidance for its members.

Emergent concepts, such as risk culture, require an iterative pathway to institutionalisation or maturity. The ABA believes that a common understanding of risk culture, and therefore the audit of risk culture, is in its early stages, and it is with this context that we make the following comments and recommendations in respect to the *Supplementary Guidance on the Audit of Risk Culture* (the **Guidance**).

Intent of the Guidance

The ABA understands the intention of the IIA is that it operate as a guide and is not mandated. It would be helpful for the IIA make explicit that the Guidance is not mandatory.

Providing flexibility

The Australian Prudential Regulation Authority's (**APRA)** Prudential Standard 'CPS 220 – Risk Management'[1] (**CPS 220**) obligates Boards to form a view on risk culture, however CPS 220 does not prescribe a standard for how Boards should go about forming their view.

In Step 3 of the ten steps ("Auditing Culture in Practice"), the Guidance suggests that the Macquarie University model is the 'baseline' for evaluating the adequacy of an organisation's risk culture (e.g., the Guidance states that "internal audit teams are encouraged to ensure that their risk culture model includes factors that reflect these four concepts at a minimum").

The ABA is concerned about the Guidance singling out one model as the preferred one – as it could bias internal auditors towards this model, instead of considering other models that may be equally robust and valid, and potentially more appropriate to organisational capacity, capability, and complexity.

[1] CPS 220 Risk Management can be accessed here https://www.apra.gov.au/risk-management

Australian Prudential Regulatory Authority (APRA)

The ABA notes that APRA has outlined risk culture as an element of its 2021 Priorities for both Supervisory and Policy activities. APRA has commenced a significant body of work to empirically test risk cultures of regulated entities, the outcome will be an Information Paper to be released later in 2021. The Information Paper will reflect APRA's expectations on risk culture, associated frameworks, and roles across 3 Lines of Defence (3LOD).

The ABA recommends the IIA liaise with APRA to ensure alignment of the Guidance to APRA's position on risk culture. It may be more expedient for the IIA to delay finalising the Guidance until the APRA expectations for risk culture are made public. Further, the Guidance should also recognise that APRA-regulated institutions will be subject to the prudential regulator's expectations in setting, governing, and auditing / reviewing risk culture.

Demarcation of 3LOD

The ABA notes that in some instances the Guidance crosses all three lines of defence. The ABA supports the observation in the guidance under the heading "2.2 Distinguishing the role of Internal Audit from other internal functions" such as clearly articulating internal audit's mandate in relation to risk culture and how it differs from the focus of other functions, with an open discussion about roles and responsibilities – while noting there is no prescribed approach.

The Guidance should explicitly recognise that some of the approaches, methodologies and techniques in the Guidance can be adopted by other functions, such as first or second line risk and compliance teams.

The Guidance should provide opportunity for different approaches to governance, including the roles of the Board-level committees – again without prescribing a particular approach.

Additions to the 10 steps

In respect to the internal audit function, the Guidance could also address the following:

- How audit can validate a risk culture model. For example, what does this process look like? What are the necessary skills for someone to validate it?
- How audit can challenge and provide assurance over Line 1/Line 2's risk culture methodology/conclusion.
- How audit can maintain independence, particularly through 'Step 10: Monitor and Review' and coordination / handoff with other business lines (e.g., Line 2, Line 1, Business, HR).

An iterative process

The ABA notes the fulsomeness of the ten-step process and considers it to be the mature state. The effort to implement the process as described in the Guidance from a standing start is very significant for some entities. It would not be reasonable to insist on the mature state as a first stage given the disparate levels of capacity and capability at banks.

Building Auditor Capability

The ABA highlights the importance of having people with the right capability to execute this work, or else following the outlined 10 steps could still produce a poor outcome (e.g., behaviourally anchored scales could be poorly developed). Therefore, we suggest that the Guidance could elaborate on the skill type required to undertake a risk culture audit.

The ABA suggests that further detail be provided on some of the recommendations to explain the reason for the recommendation and to provide further information for consideration. This way, if an audit team decides that they cannot action a recommendation they understand the potential disadvantages or risks of not doing so.

The ABA thanks you for the opportunity to provide feedback on the Guidance and welcomes further discussion should clarification of any matters noted here be required.

Kind Regards

Emma Penzo
Policy Director
Emma.Penzo@ausbanking.org.au